

Malwarebytes Endpoint Security

Advanced threat prevention

核心技術

Anti-malware

- 預防先進的惡意軟體攻擊

Anti-exploit

- 四層的漏洞防護裝置

Anti-ransomware

- 自動偵測及阻止勒索軟體

Management console

- 安全策略、中央監控以及即時回報

獲得獎項



美國最具潛力公司



年度最佳產品



年度創新安全獎

Malwarebytes Endpoint Security 是運用多重防護技術主動防禦用戶電腦避免受到未知和已知威脅的端點保護平台。

提供多階段的攻擊防護，讓全球所有行業及各種規模的公司，均能阻止網路犯罪者的攻擊。

主要優點

阻止先進的惡意軟體及勒索攻擊

面對傳統安全防護無法阻擋的惡意軟體及資料外洩，提供優秀的防護能力，節省 IT 資源。

防護漏洞及勒索軟體

通過漏洞防護來保護系統不再支援更新的程式。無特徵碼監控技術自動檢測及阻止未知、零時差攻擊(Zero-hour) 的勒索軟體。

提高生產力

維持終端用戶系統效能，保持系統效能和提高員工的生產力。

擴展威脅預防

伴隨著公司發展，擴展部署至每一端點的保護和範圍。

偵測未受保護的系統

偵測網路上的所有未受保護的端點和軟體，透過系統派送安裝獲得保護。

修復 Mac 端點

快速檢測並清除 OS X 終端上的惡意軟體，包括廣告軟體。*

*Mac 用戶無法使用管理平台控管，也無法提供即時防護。



Anti-malware

- 主動反惡意軟體/反間諜軟體掃描
- 三種系統掃描模式(快速/Flash/全面掃描)
- 惡意網站攔截
- 執行檔運行攔截
- Malwarebytes 變色龍隱匿技術
- 重啟系統後刪除檔案(可選擇)

Anti-exploit

- 防止嘗試繞過作業系統保護
- 防止利用代碼從特定或特定內存區域執行
- 應用行為保護
- 應用程式強化

Anti-ransoware

- 即時偵測，攔截加密引擎
- 專有的勒索軟體行為判斷技術
- 無特徵碼技術鑑定未知及零時差勒索軟體
- 不耗系統資源
- 與第三方安全解決方案兼容

Management Console

- 具派送安裝功能的擴點管理
- 靈活的掃描排程設定
- 中央報告查看威脅資訊
- 虛擬部署模擬器
- AD 應用整合

作業系統需求

用戶端

支援的操作系統

Windows 10、8.1、8、7、Vista、XP

Windows Server 2016、2012、2008、2003

Windows Small Business Server 2011

Mac OS X (10.8 或更新的版本)

硬體設備

800 MHz CPU 或更快的 CPU

1 GB RAM 或以上(Windows Server 需要 2 GB 或以上)

35 MB 可用儲存空間

中控管理台

支援的操作系統

Windows Server 2016、2012、2008

支援的 Microsoft SQL Server

SQL Server 2016、2014、2012、2008

SQL Server 2008 Express (包含產品)

硬體設備

2 GHz CPU(建議雙核心 2.6 GHz 或更快的 CPU)

2 GB RAM 或更高 (建議 4 GB)

10 GB 可用儲存空間 (建議 20 GB)

